ANÁLISIS DE RIESGOS DE CIBERSEGURIDAD EN ARQUITECTURA DE VEHICULOS AUTOMATIZADOS

[1,2]Leonardo González, [2]Myriam Vaca, [2]Ray Lattarulo, [1]Isidro Calvo, [2]Joshue Pérez, [2]Alejandra Ruiz
{leonardo.gonzalez , myriam.vaca, ray.lattarulo, joshue.perez, alejandra.ruiz}@tecnalia.com,
isidro.calvo@ehu.eus
[1]Universidad del País Vasco
[2]Tecnalia Research and Innovation

Resumen

Los vehículos conectados y automatizados han sido recientemente concebidos como entes ciberfísicos, estrechamente relacionados con la red del Internet de las cosas (IoT). Este hecho supone un incremento en la superficie de ataque del vehículo, que junto a la creciente tendencia hacia vehículos automatizados, hacen que estos riesgos de ciberseguridad puedan tener consecuencias catastróficas en seguridad vial. En el presente trabajo se expone un análisis de riesgos de ciberseguridad en el marco de una arquitectura de vehículos automatizados. Este análisis previo se realiza en el contexto de dos escenarios de estudio en maniobras cooperativas. Inicialmente se presenta un estado del arte de la ciberseguridad en automoción, así como también su repercusión en entornos automatizados, haciendo especial énfasis en las comunicaciones entre vehículos y con infraestructura. Además, se analizan dos maniobras cooperativas, y se ilustran una serie de posibles ataques en la plataforma.

Palabras clave: ciberseguridad, vehículos automatizados, seguridad, maniobras cooperativas.

1. Introducción

Las tecnologías de información y comunicación lideran el avance en la era digital, así mismo forman parte importante del desarrollo de sistemas inteligentes de transporte (SIT). Los SIT ofrecen la oportunidad de mejorar la seguridad de transporte, reducir el impacto ambiental y favorecer la productividad y eficiencia a través de la integración de sistemas de comunicación y percepción en vehículos inteligentes.

El desarrollo de sistemas de comunicaciones en vehículos para la mejora de la eficiencia y la modernización de la infraestructura de transporte ha sido un foco importante en el área automotriz. Sin embargo, recientemente con el auge del vehículo automatizado, la comunicación vehicular supone también un agregado de seguridad a estos sistemas, previendo obstáculos no visibles para un coche, o previniendo de eventualidades en la vía, invisibles al rango de visión de la sensórica del vehículo.

En la actualidad la mayoría de los fabricantes ya ofrecen algún nivel de automatización a través de una serie de sistemas ADAS (Advanced Driver-assistance Systems). Estos disminuyen los riesgos en la vía mediante la automatización de algunas tareas de conducción y prevención de colisiones, y pueden ser considerados sistemas nivel 2, de acuerdo al estándar SAE J3016.

Los vehículos conectados son un ente ciberfísico; una red de elementos interconectados, con múltiples unidades de control electrónico (ECU) con comunicación intra-vehicular, comunicaciones externas con infraestructura inteligente, otros vehículos e inclusive Internet. Esta expansión en las capacidades de comunicación del vehículo genera un incremento en la superficie de ataque, en cuanto a riesgos de seguridad informática se refiere.

En este trabajo se presenta un estudio breve sobre ciberseguridad en los vehículos automatizados y conectados, y su repercusión en el riesgo vial. Además, se realiza un análisis más detallado de estos riesgos sobre la arquitectura de vehículos automatizados propuesta en [1]. Adicionalmente se proponen dos casos de estudio de maniobras cooperativas.

El resto del artículo esta distribuido de la siguiente forma: en la sección 2 se realiza un resumen del estado del arte en la ciberseguridad y la relación con riesgos en vehículos automatizados. En la sección 3 se presenta la arquitectura mencionada antes junto a su respectivo análisis en el entorno de ciberseguridad y se describe la plataforma de pruebas. En la sección 4 se explican los casos de estudio propuestos en conducción cooperativa para validar la arquitectura de vehículos automatizados, y se ilustran posibles escenarios de ataque. Finalmente, en la sección 5 se presentan las conclusiones del trabajo realizado y posibles trabajos futuros.

2. Estado del arte

2.1. Riesgo en vehículos automatizados

La gestión de riesgos constituye una parte importante de la arquitectura de un vehículo inteligente, y asegurar el correcto funcionamiento de sus partes permanece como un reto en las metodologías de validación y verificación. Esto conlleva que en la actualidad las simulaciones de situaciones complejas en escenarios de conducción cooperativa [2] supongan un foco de estudio importante.

Sin embargo la habilidad de un coche para evaluar en tiempo de ejecución riesgos en la vía se ha vuelto un punto importante de investigación [3]. En [4] se comparan diferentes indicadores de riesgos, y se asocian con la capacidad del sistema de estimar correctamente estados futuros.

La estimación de estados futuros, se traduce en la capacidad predictiva del vehículo, la cual proviene de un concepto de modelo de sí mismo, y de los demás participantes en la vía. Dicho modelo, puede ser un modelo físico en base a una serie de características, o un modelo estadístico proveniente de datos experimentales [5]. Recientemente se han estudiado una serie de colisiones provenientes de vehículos automatizados, haciendo análisis de informes de fabricantes, y sistemas de conducción asistida en [6]

2.2. Riesgo en vehículos conectados

Los vehículos conectados, si bien proporcionan al vehículo mejor capacidad predictiva incrementan el riesgo del vehículo ante un ciberataque, al integrar datos fuera del rango de la sensórica. Este riesgo de seguridad, puede tener repercusiones graves, respecto de los riesgos en la vía.

Este nuevo vector de ataque, debe ser manejado de forma apropiada, para reducir la superficie vulnerable a un ciberataque. Para ello es necesario desde un punto de vista de diseño, disponer de un perfil de posible atacante, y un plan basado en mejores prácticas para ciberseguridad.

Esta relación entre seguridad del vehículo y sus funciones, y ciberseguridad (*safety and cybersecurity*), ha sido estudiada previamente en [7]. En [8] se implementan pseudónimos con la finalidad de proteger la privacidad en la red y su impacto sobre las aplicaciones V2X (del inglés *vehicle-to-everything*, que se refiere a las comunicaciones entre un vehículo y cualquier otra entidad.).

2.3. Relación entre *cybersecurity* y *safety*

Los vehículos son sistemas de seguridad crítica (*Safety critical systems*) siendo así los riesgos asociados a estos sistemas de grave repercusión para las personas o el ambiente, y pudiendo causar daño irreparable. Al ser este tipo de sistemas cada vez más interconectados, la ciberseguridad tiene un papel relevante en asegurar que el sistema sea robusto ante posibles ataques. En [9] se hace un estudio de la dualidad entre *safety* y *cybersecurity* en entornos industriales, se comparan los métodos utilizados para el desarrollo de ambas disciplinas y su clasificación. Al momento de diseñar estos sistemas, independientemente de la metodología utilizada, identifican la ciberseguridad y la seguridad, como ramas interdependientes.

En [10], la Sociedad de Ingenieros de Automoción (SAE) presenta una guía para el desarrollo de ciberseguridad en vehículos. El foco principal del presente trabajo, se encuentra en el punto común de estas ramas de estudio; la ciberseguridad, y la seguridad del vehículo (*safety*), y es importante recalcar que no todas las amenazas de ciberseguridad suponen riesgos en sistemas críticamente seguros, por ejemplo; un posible ataque al sistema , no supone un riesgo para el vehículo, pero sí concierne a la privacidad del conductor.

Una serie de posibles ataques han sido estudiados en vehículos automatizados, en [11] se presenta un resumen de una serie de ataques potenciales sobre infraestructura en la vía, sensórica, mapas internos del vehículo, comunicaciones internas del vehículo (CAN principalmente) y comunicaciones con otros entes en entornos cooperativos. Además, las consecuencias y clasificación de estos ataques se presentan en forma de riesgos altos, medios y bajos.

2.4. Ciberseguridad en vehículos

La seguridad en el vehículo moderno toma cada vez más relevancia con el incremento de sus capacidades de comunicación. Sin embargo, las redes internas de los vehículos son un foco importante al momento de analizar los riesgos de seguridad. En [12] se realiza un análisis teniendo en cuenta los principales buses de comunicación entre ECUs. Un estudio sobre el impacto de posibles ataques de seguridad en vehículos automatizados es presentado en [11].

Vulnerabilidades

Las vulnerabilidades en la red vehicular pueden ser clasificadas de acuerdo a su ubicación en la arquitectura de la red, la infraestructura que sufre el ataque y el atacante. En [13] se dividen en

función de la capa: ataques en capa de aplicación, red y sistema. En [11] estos ataques se clasifican de acuerdo a la arquitectura en particular afectada, y se hace una diferenciación entre vehículos automatizados y conectados.

Atacante

Definir una serie de propiedades de un posible perfil de atacante, es útil al momento de crear estrategias de seguridad. En el caso de redes vehiculares en [14] se identifican cuatro dimensiones: ubicación, intenciones, alcance y actividad. La ubicación se refiere a si el atacante es externo o interno a la red. Las intenciones tienen que ver con la predictibilidad del atacante y pueden ser racionales o maliciosas. El alcance puede ser local o global dependiendo de los entes afectados, y finalmente, el atacante puede ser activo o pasivo, en función de su actividad en la red.

En un informe publicado por Intel en [15], se identifican además una serie de posibles grupos, con características similares a las descritas anteriormente. Adicionalmente en [16] se añade a las dimensiones anteriores la adaptabilidad de un atacante, siendo este estático o adaptativo y se propone una posible clasificación del atacante.

Definición de escenario

La superficie de ataque en un vehículo moderno incluye comunicaciones internas y externas. El trabajo realizado por [17], detalla una serie de estrategias destinadas a cubrir posibles ataques en ambos frentes. Sin embargo, el entorno cooperativo supone una serie de riesgos asociados directamente a la maniobra cooperativa. Cada maniobra cooperativa debe ser identificada y asociada a una serie de estados seguros, ante la eventualidad de un posible ataque.

En [13] se analiza el caso de un CACC (del inglés *Cooperative Automated Control Cruise*) ante ataques de seguridad al canal de comunicación, y se presenta una serie de posibles estrategias para remediar y minimizar el impacto de estos.

3. Plataforma y Arquitectura

La actual plataforma tiene como foco la realización y desarrollo de herramientas para la conducción automatizada. Se encuentra estructurada en una serie de bloques que proporcionan modularidad al sistema y permiten abstraer funcionalidades, para mantener el sistema escalable y adaptable.

Actualmente la arquitectura propuesta, se constituye de 6 bloques: Adquisición, percepción, decisión, control, actuación y comunicaciones [1]. Cada uno de estos bloques a su vez tiene una serie de responsabilidades, sobre la funcionalidad final del vehículo, y mantiene comunicación con los demás bloques del sistema.

En el marco del estudio de riesgos provenientes de redes de vehículos, los bloques más relevantes son decisión y comunicaciones. El bloque de comunicaciones debe hacer uso de una serie de protocolos, que permitan la correcta inferencia del estado de la vía, y que sirvan para alertar al conductor, de otros vehículos así como de eventualidades. Todo ello sin exponer el vehículo a posibles ataques o vulnerabilidades de privacidad.

Las comunicaciones pueden ser vistas, de esta forma como complementarias a los sistemas de percepción que provee la sensórica, con la ventaja, de que su percepción espacial no se encuentra tan limitada, pudiendo establecer así comunicaciones con vehículos sin necesidad de tener línea de vista.

Esta ventaja de los sistemas de comunicación hace que sean muy valiosos para la consecución de vehículos automatizados de alto nivel. Además los vehículos conectados pueden ser percibidos como un sistema distinto, el cual permite el establecimiento de maniobras cooperativas. Ello quiere decir que, dadas las condiciones correctas, un sistema de vehículos conectados podrían establecer maniobras cooperativas que por seguridad serían imposibles de realizar en un entornos sin comunicaciones.

Por ejemplo en el caso de *platooning* se podrían corregir las consecuencias del llamado efecto de acordeón y se reducirían las distancias (espacial o temporal) de seguridad entre coches, sin aumentar el riesgo que a ello supone en entornos sólo basados en percepción.

Sin embargo, añadir conectividad al coche, hace que la superficie de ataque crezca. El vehículo moderno, es una plataforma ciberfísica, con múltiples ECUs comunicándose entre sí, sistemas de información, buses de control de bajo nivel, entre otros. Esta arquitectura de red interna, se ve incrementada ahora, por la comunicación con una red de vehículos (V2V) e infraestructura (V2I).

3.1. Plataforma de pruebas

A continuación se realizará una presentación del vehículo real, el sistema de simulación que se utilizará para la implementación de los casos de uso, la arquitectura en la que se basan y la estación central.

- El vehículo real se corresponde a un Renault Twizy 80 eléctrico, cuya máxima velocidad

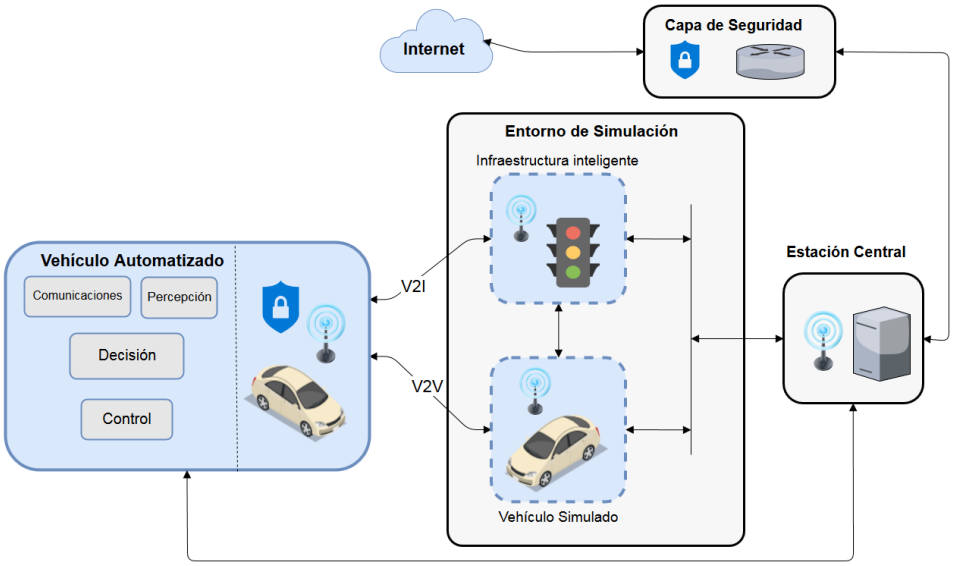


Figura 1: Arquitectura de comunicaciones.

es de $80Km/h$. Su instrumentación permite el control automático del vehículo controlando los principales actuadores, el volante y los pedales de acelerador y freno, mediante una red de Bus CAN por un Controlador de Lógica Programable (PLC). Una descripción detallada de como está implementada la arquitectura del vehículo se puede encontrar en [18]. Además, el vehículo está equipado con un DGPS-RTK para el posicionamiento, sensores láser para reconocimiento de obstáculos y cámaras para detección de señales y peatones. Así mismo, consta de inteligencia integrada para la planificación de rutas en tiempo real y controladores laterales y longitudinales; y de dispositivos de comunicación para V2X. Por último, consta de un ordenador a bordo encargado de correr los algoritmos y gestionar las comunicaciones.

- Para la simulación del vehículo se utiliza Dynacar, una herramienta desarrollada por Tecnalia Research and Innovation (ver Figura 2). Este simulador proporciona un modelo de alta precisión de un vehículo, con un marco integrado en un entorno de simulación Matlab/Simulink para la ejecución en tiempo real de funcionalidades automatizadas. Se centra principalmente en la dinámica basándose en un modelo de vehículo multicuerpo combinado con el modelo de neumático Pacejka y submodelos para elementos como motor, transmisión, sistema de dirección, sistema de frenado, etc. Además, Dynacar permite una buena definición de trayectorias, maniobras cooperativas y validación virtual con varios y diferentes tipos de vehículos en escenarios complejos y personalizables [1].

Figura 2: Herramienta de simulación Dynacar

- El marco general de la estructura utilizada para la conducción automatizada se basa en una arquitectura modular formada por seis bloques correspondientes a Adquisición, Percepción, Comunicación, Control, Decisión y Actuación. Este marco se ha utilizado en el pasado para varias aplicaciones de manejo automatizado tales como: validación de controladores longitudinales [18], comparación de controladores laterales [1], maniobras de adelantamiento [19] y diferentes enfoques de planificador de velocidad [20]. Así pues, a continuación se describirán sólo los bloques que interfieren directamente.

    - Comunicación: Ofrece un flujo de información bidireccional con plataformas externas como vehículos (V2V), infraestructura (V2I) y otro tipo de dispositivos tecnológicos (V2X), para alcanzar un entorno de manejo cooperativo que permita

maniobras más seguras y cómodas. Esta comunicación se lleva a cabo mediante redes W-Lan.

- Decisión: Este módulo decide el comportamiento dinámico del vehículo, es decir, se encarga de cálculos tales como: planificadores de velocidad longitudinal, trayectos libres de obstáculos y activación de maniobras seguras (adelantamiento, frenado de emergencia, etc). Esto permite reaccionar ante situaciones inesperadas que generalmente afectan el escenario de conducción predefinido.

- Por último, la estación central está destinada a controlar el comportamiento de los vehículos en todo momento procesando la información que se recibe de ellos, y envía las instrucciones correspondientes a cada vehículo para controlar la ejecución de la maniobra. Esta estación consta de información de base de GPS diferencial, HMI para vigilancia, cobertura WiFi, un dispositivo de comunicación V2X y una computadora en la que se ejecutará Dynacar.

3.2. Riesgo en la Arquitectura de Vehículos Automatizados

En la arquitectura de vehículos automatizados presentada en [1], se reconocen los bloques de adquisición y comunicaciones como los principales bloques susceptibles de recibir un ataque. Por su parte, el bloque de decisión al ser responsable del plan a realizar por el vehículo y la realización de diferentes maniobras, es el principal encargado de prevenir posibles fallos y establecer estados seguros ante un posible mal-funcionamiento.

En el bloque de adquisición, las vulnerabilidades se encuentran en la sensórica, siendo ésta susceptible a ataques de denegación de acceso (DoS), los cuales para sensores de odometría pueden ser atacados a través de campos magnéticos y, en el caso de sensores ópticos, la utilización de material reflectivo o absorbente. Además, este bloque también comprende la comunicación con buses dentro del vehículo, intervenciones en el protocolo CAN a través del puerto OBD, pudiendo inyectar o modificar la estructura de mensajes directamente relacionados con el control de las ECU en el vehículo.

Estos ataques dependiendo de la robustez de los sistemas y la sensórica del vehículo pudieran tener repercusiones graves en la seguridad, inhabilitando así su capacidad de percibir obstáculos, o generando obstáculos que no se encuentran en la vía, enviando comandos errados o simplemente entorpeciendo las comunicaciones entre ECUs.

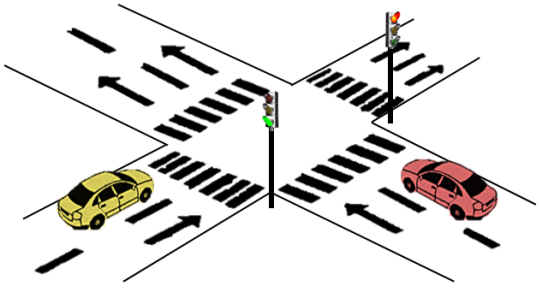
Sin embargo la superficie de ataque mas extendida, y que supone mayor riesgo, es la de las comunicaciones. En el caso de ataque en el bloque de adquisición, la presencia física del ente atacante es casi siempre necesaria, no así en un vehículo perteneciente a una red vehícular, o directamente conectado al Internet.

La modificación de información satelital proveniente de GPS supone un riesgo elevado dentro de esta categoría, comprometiendo la capacidad del coche de localizarse. Las comunicaciones V2X, suponen un incremento en la seguridad vial al proveer de redundancia y constante posicionamiento de sus actores, sin embargo, desde el punto de vista de ciberseguridad suponen una serie de retos. El constante envío en modo *broadcast* de mensajes en la vía, hace que la privacidad del vehículo se vea comprometida. Algunas soluciones se han propuesto respecto del uso de pseudónimos, sacrificando algunos beneficios de seguridad [8]. Un mensaje V2V errado o proveniente de un vehículo inexistente podría poner en peligro al vehículo receptor, al realizar una maniobra incorrecta. De igual forma en el caso de mensajes V2I, la incorrecta interpretación de una señalización, o un ataque de denegación de acceso, debe considerarse como un riesgo crítico.

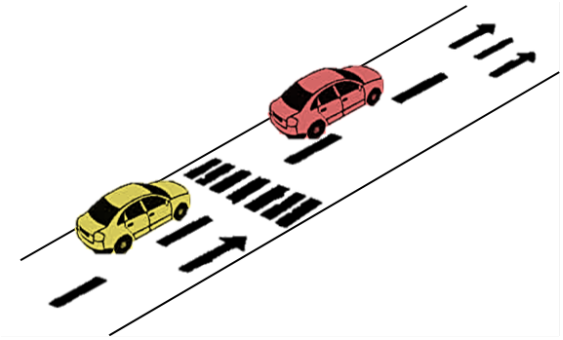
4. Casos de Estudio

A continuación se presenta el caso de uso en el marco del proyecto europeo, SerIoT (*Safety and Security for the Internet of Things*). En este caso, se refiere al análisis y definición de soluciones de seguridad para aplicaciones de SIT integradas en el amplio contexto de las ciudades inteligentes (*Smart Cities*). Una de las principales actividades de estandarización en SIT es la especificación de la comunicación V2X, para que se intercambie información de manera segura siguiendo el protocolo ITS-G5 en Europa.

Los escenarios presentados en este artículo hacen uso de un vehículo automatizado, una estación central, y una serie de entidades simuladas, con la finalidad de validar maniobras cooperativas, en concreto, un *platooning*, y un cruce inteligente como se muestran en la figura 3. Así pues, su actuación se basa en el intercambio de información entre vehículos (Vehicle-to-Vehicle communication, V2V) o con una estación central(Vehicle-to-Infrastructure communication, V2I). Esta estación central monitoriza el comportamiento del vehículo en todo momento, procesando la información recibida y enviando las instrucciones correspondientes para cada vehículo y controlando la ejecución de la maniobra.



(a) Cruce inteligente



(b) textitPlatooning basado en CACC.

Figura 3: Caso(s) de uso. Platooning y cruce.

En este contexto, es importante el desarrollo de una comunicación V2X robusta y segura contra ciberataques y amenazas, asegurando así que la evolución de los SIT se realiza sin riesgos de seguridad o vulnerabilidades. Con ello además, se garantiza la seguridad de los pasajeros ya que, una violación de seguridad puede generar no sólo pérdida de datos, sino también accidentes de tráfico que lleven a consecuencias graves.

En el caso del platooning, se desarrollará con un vehículo líder que circula en modo manual. Éste definirá el perfil de velocidad, acelerando y frenando de forma no regular. Se añadirán uno o varios vehículos, que se corresponden a coches simulados circulando en modo semiautomático, que seguirán al vehículo líder en cadena a una distancia de seguridad definida.

Por lo tanto, la estación central podrá simular diferentes situaciones complejas y de riesgo en las que un vehículo virtual no respeta la distancia mínima de seguridad con respecto a los otros vehículos, la aparición de obstáculos, etc. Así pues, cada vehículo puede transmitir y recibir información hacia y desde el resto y la estación central.

Para el cruce inteligente, la base central mandará información sobre el estado de los semáforos correspondientes para cada vehículo, de tal forma que, cada uno modifique el perfil de velocidad y se realice el cruce de forma segura sin necesidad de que ninguno de los vehículo deba detenerse. Esta maniobra se ejecutará con un coche real y uno simulado.

Al ser la estación central el principal ente de control en ambas maniobras, los vectores de ataque a estudiar se focalizan sobre ésta. En principio un posible ataque podría modificar la integridad del mensaje, o incrementar la latencia de respuesta, dificultando el establecimiento de maniobras cooperativa. Para ello la caracterización del protocolo de comunicación, permitiría reconocer patrones relacionados con la maniobra, y prevenir posibles intervenciones.

Cabe destacar que cada mensaje V2X debe recibirse con una cierta periodicidad, cumpliendo la frecuencia mínima especificada en el Estándar ETSI TR 102 638 [21], y con una latencia dentro del tiempo de latencia máxima especificado también en [21]. De lo contrario, la estación central generará un mensaje de advertencia.

La estación central analizará la información proveniente de los vehículos y los nodos implementados en la red SerIoT, gestionando la detección de las diferentes situaciones anormales que provocan que la maniobra seleccionada no esté funcionando como se esperaba, por ejemplo, que la distancia mínima de seguridad entre los vehículos no se mantiene o que la velocidad en el cruce no se regula correctamente. Así mismo se verifica que ninguna de las comunicaciones basadas en V2X esté siendo pirateada.

Si el ataque o fallo es detectado y confirmado, la estación informa de la situación y actúa en consecuencia con la solución que crea conveniente para alcanzar un modo de conducción segura. En el caso de que la maniobra no se corresponda con la esperada, la estación modifica los parámetros de configuración de los vehículos y corrige la maniobra. Por otro lado, si se refiere a un ataque, se deshabilita la maniobra y se ignora la información recibida posterior al ataque hasta que sea neutralizado. Mientras eso pasa, los vehículos proceden a realizar una maniobra para alcanzar un estado de conducción seguro, por ejemplo, re-planificación de rutas o de velocidad, frenado de emergencia, cambio en el perfil de velocidad, entre otras soluciones.

Los objetivos a alcanzar con estos casos de uso son los siguientes:

1. Facilitar la detección temprana de fallos y/o errores al verificar minuciosa y repetidamente ciertos casos sin restricción de tiempo o perturbaciones ambientales.

2. Minimizar los efectos de los ciberataques y las amenazas mediante el uso de la solución de se-

guridad IoT propuesta en el proyecto SerIoT, garantizando así comunicaciones seguras y robustas basadas en V2X.

3. Validar diferentes maniobras cooperativas entre vehículos, basados en comunicaciones V2V y V2I y evaluar el impacto que el esquema de seguridad de SerIoT tenga sobre estas.

5. Conclusión y trabajos futuros

Las nuevas tecnologías de comunicación vehicular en conjunto con el avance de vehículos automatizados, trae consigo una serie de problemáticas desde el punto de vista de seguridad. Vulnerabilidades sobre vehículos conectados han sido demostradas previamente, teniendo consecuencias económicas importante sobre los fabricantes en el pasado. Sin embargo, el potencial de explotar vulnerabilidades sobre vehículos altamente automatizados supone nuevos riesgos.

El presente trabajo realiza una revisión sobre el estado del arte, y los ataques reportados de forma pública en los últimos años, y presenta un análisis de riesgos de ciberseguridad en una arquitectura de vehículos automatizados.

A su vez se exponen algunas de las posibles vulnerabilidades, y un caso de estudio experimental que incluye dos escenarios de maniobras cooperativas. Este trabajo es un estudio preliminar, con la finalidad de validar y verificar maniobras seguras en el marco de un posible ataque de ciberseguridad.

En futuros trabajos, se buscará establecer una arquitectura de red, que permita en el marco de IoT, asegurar la comunicación en redes vehículares de entes externos, su verificación a través de entornos de simulación y su validación en plataformas reales. También es necesaria la caracterización de un protocolo y mejores prácticas en el entorno de la ciberseguridad, así como la caracterización de maniobras específicas relacionadas con posibles fallos o ataques, para garantizar un sistema robusto.

Agradecimientos

Los autores quieren agradecer al proyecto H2020 SerIoT (número de subvención 780139) por brindar los recursos para el desarrollo del siguiente artículo.

English summary

CYBERSECURITY RISK ANALYSIS IN AUTOMATED VEHICLE ARCHITECTURE

Abstract

Connected and automated vehicles have been recently categorized as cybephysical entities, tightly related with a part of the Internet of Things (IoT) network. As a consequence the attack surface of a modern vehicle is increased, which added to the automation trend, makes cibersecurity risks a higher threat in the road. In this work a framework for automated vehicles is described, with the objective of validating security strategies when performing cooperative maneuvers. A review of the state of the art in automotive cibersecurity is presented, along its effect in automated vehicles, making special emphasis in inter-vehicle (V2V) communication and to the infrastructure (V2I). Moreover, two maneuvers are studied and a series of safety factors, taking into consideration the posible intervention of external malicious agents.

Keywords: cybersecurity, automated vehicles , safety, cooperative maneuvers.

Referencias

[1] R. Lattarulo, J. Pérez, and M. Dendaluce, "A complete framework for developing and testing automated driving controllers," *IFAC-PapersOnLine*, vol. 50, pp. 258–263, jul 2017.

[2] I. Jemaa, P. Cincilla, A. Kaiser, and B. Lonc, "An Overview of Security Ongoing Work in Cooperative ITS," jun 2017.

[3] C. Katrakazas, M. Quddus, W.-H. Chen, and L. Deka, "Real-time motion planning methods for autonomous on-road driving: State-of-the-art and future research directions," *Transportation Research Part C: Emerging Technologies*, vol. 60, pp. 416–442, 2015.

[4] S. Lefèvre, D. Vasquez, and C. Laugier, "A survey on motion prediction and risk assessment for intelligent vehicles," *ROBOMECH Journal*, vol. 1, no. 1, p. 1, 2014.

[5] M. Althoff and A. Mergel, "Comparison of Markov chain abstraction and Monte Carlo simulation for the safety assessment of autonomous cars," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1237–1247, 2011.

[6] F. M. Favarò, N. Nader, S. O. Eurich, M. Tripp, and N. Varadaraju, "Examining accident reports involving autonomous vehicles in California," *PLOS ONE*, vol. 12, p. e0184952, sep 2017.

[7] J. Nilsson, C. Bergenhem, J. Jacobson, R. Johansson, and J. Vinter, "Functional Safety for Cooperative Systems," *SAE Technical Papers*, vol. 2, no. April, 2013.

[8] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," *IEEE Vehicular Networking Conference, VNC*, pp. 71–78, 2013.

[9] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering and System Safety*, vol. 139, pp. 156–178, 2015.

[10] SAE, " Cybersecurity Guidebook for Cyber-Physical Vehicle Systems ," standard, Society of Automotive Engineers, Jan. 2016.

[11] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[12] M. Wolf, A. Weimerskirch, and C. Paar, "Security in Automotive Bus Systems," *Proceedings of the Workshop on Embedded Security in Cars*, no. July, pp. 1–13, 2004.

[13] M. Amoozadeh, A. Raghuramu, C.-n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, pp. 126–132, jun 2015.

[14] M. Raya, M. Raya, J. Hubaux, and J. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39–68, 2007.

[15] Intel, "Automotive Security Best Practices," *Whitepaper*, p. 19, 2015.

[16] A. Panchenko and L. Pimenidis, "Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication," pp. 240–251, 2006.

[17] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications*, vol. 10, pp. 13–28, oct 2017.

[18] M. Marcano, J. A. Matute, R. Lattarulo, E. Martí, and J. Pérez, "Low Speed Longitudinal Control Algorithms for Automated Vehicles in Simulation and Real Platforms," *Complexity*, vol. 2018, pp. 1–12, mar 2018.

[19] R. Lattarulo, M. Marcano, and J. Pérez, "Overtaking Maneuver for Automated Driving Using Virtual Environments," pp. 446–453, 2018.

[20] R. Lattarulo, E. Marti, M. Marcano, J. Matute, and J. Perez, "A Speed Planner Approach Based On Bézier Curves Using Vehicle Dynamic Constrains and Passengers Comfort," 2018.

[21] "INTELLIGENT TRANSPORT SYSTEMS (ITS); VEHICULAR COMMUNICATIONS; BASIC SET OF APPLICATIONS; DEFINITIONS," standard, ETSI TR 102 638, 2009.